Lecture 5

Now that we have seen what a subgroup is, the next question is to be able to check whether a subset H of a group G is a subg-roup or not. Well, the first thing we definitely need is that the identity element is in H, otherwise we can rule out the possibility of H being a subgroup.

If we follow the definition of a group, then we need to check 4 things to make sure that H is a subgroup. Here is a test which makes the work a little bit less.

Theorem [The Subgroup test]

Let $(G, \cdot)$ be a group and H be a non-empty subset of G. Then $H \leq G$ if the following two conditions hold :-

1. For all $a, b \in H$, $a \cdot b \in H$ and
2. For all $a \in H$, $a^{-1} \in H$.

Proof. To check that H is a group in itself under '$\cdot$', we need to check that the operation '$\cdot$' is a binary operation on H, the existence of identity, associativity and the existence of inverse.

Condition 1) in the theorem guarantees that '$\cdot$' is a binary operation on H.

Since G is a group, we know that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall$ $a, b, c \in G$ and so in particular, is true for all $a, b, c \in H$.

For showing the existence of identity in H, choose $a \in H$ (as $H \neq \phi$). Now condition 2) tell us that $a^{-1} \in H$. Again, by condition 1), '$\cdot$' is a binary operation on H and so, $a \cdot a^{-1} = e \in H$.

Finally, condition 2) is precisely the existence of inverse.

$\boxed{//}$

Before moving to cyclic groups, let's see two special subgroups of a group.

<u>Definiton</u> Center of a group

The center of a group G, denoted by $Z(G)$ is the subgroup of G which commutes with every element in G, i.e.,

$$Z(G) = \{ a \in G \mid ax = xa \text{ for all } x \in G \}$$

Remark If G is non-abelian then $Z(G) \neq G$.

Exercise Prove that $Z(G)$ is a subgroup of G.

e.g. 1) If $G = D_4$, then one can check that $Z(G) = \{R_0, R_{180}\}$

So for finding the center of a group, find all the elements in the group which commutes with all other elements.

Definition Centralizer of a in G

Let G be a group and $a \in G$ be a fixed element in G. The centralizer of a in G is the set of all elements in G which commute with a, i.e.

$$C(a) = \{g \in G \mid ga = ag\}$$

Exercise Prove that $C(a) \leq G$, $\forall\, a \in G$.

e.g. Again let $G = D_4$, then

$$C(R_0) = D_4 = C(R_{180})$$

$$C(R_{90}) = \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270})$$

$$C(H) = \{R_0, H, R_{180}, V\} = C(V)$$

$$C(D) = \{R_0, D, R_{180}, D'\} = C(D')$$

Cyclic Groups

Now that we have studied about subgroups, let's study for a while, about a very important class of groups - cyclic groups.

First recall, that a subgroup generated

by a single element $a \in G$, denoted by $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. Now a question arises, is it possible that the whole group can be generated by a single element.

Let's see some examples: $\rightarrow$

i) $(\mathbb{Z}, +)$. I claim that $\langle 1 \rangle = \mathbb{Z}$ (Recall that $1^k = \underbrace{1 + \cdots + 1}_{k\text{-times}} = k$ in $(\mathbb{Z}, +)$).

Now, given any $n \in \mathbb{Z}$, we can write $n = \underbrace{1 + \cdots + 1}_{n\text{-times}}$ if $n > 0$ and $n = \underbrace{(-1) + \cdots + (-1)}_{n\text{-times}}$ if n is negative. In any case, all the elements of $\mathbb{Z}$ can be written as a power of 1 and so $\mathbb{Z}$ is generated by a single element $\{1\}$.

Remark :→ By the argument, same as above, one can show that $\langle -1 \rangle = \mathbb{Z}$ too, so a group can be generated by more than one elements.

ii) Consider $(\mathbb{Z}_5, +)$. Again $\mathbb{Z}_5 = \langle 1 \rangle$ as any element of $\mathbb{Z}_5$ can be written as a power of 1.

iii) Consider $U(9)$, the group of units in $\mathbb{Z}_9$, under multiplication in $\mathbb{Z}_9$. Then

$$U(9) = \{1, 2, 4, 5, 7, 8\}$$

Claim :- $U(9) = \langle 2 \rangle$

Proof of the Claim :- Let's just see what $\langle 2 \rangle$ in $U(9)$ is. For that we'll have to see the powers of 2, keeping in mind the fact that the multiplication is modulo 9.

$$2^0 = 1$$
$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 = 16 = 7 \mod 9$$
$$2^5 = 32 = 5 \mod 9$$

So we got all the elements in $U(9)$. Can we have more? You can check that if we start taking more powers of 2, the above pattern starts repetating itself.

Ques :- What is $\langle 4 \rangle$ and $\langle 5 \rangle$ in $U(9)$?

<u>Exercise</u> :- Suppose I tell you that above three are examples of cyclic groups. Try to make a definition of a cyclic group.